OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

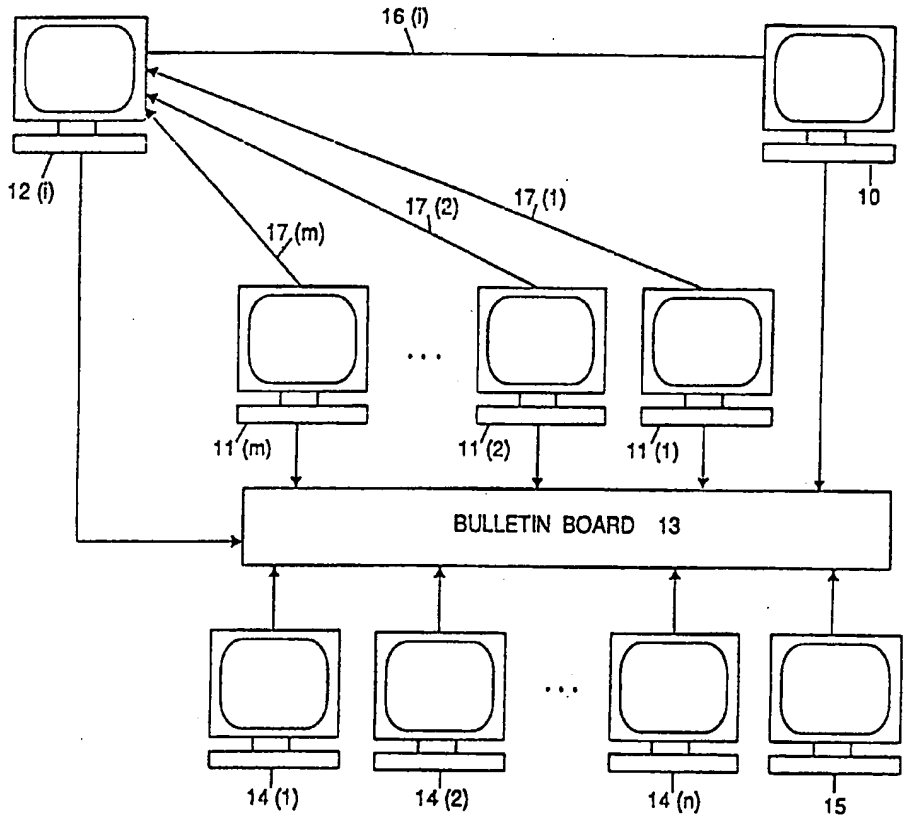
(12) (19) (CA) **Brevet-Patent**

(11) (21) (C) **2,176,990**
(22) 1996/05/21
(43) 1996/11/20
(45) 2000/05/16

(72) Kilian, Joseph J., US
(72) Sako, Kazue, JP
(73) NEC CORPORATION, JP

(51) Int.Cl.[6] G07C 13/00
(30) 1995/05/19 (08/444,701) US

(54) **VOTE ELECTRONIQUE SUR**
(54) **SECURE RECEIPT-FREE ELECTRONIC VOTING**



(57) A number-theoretic based algorithm provides for secure receipt-free voting. A vote generating center generates a choice of votes for each voter or vote chooser. The votes are encrypted, shuffled, and conveyed to a vote chooser along with information regarding how the votes were shuffled without being intercepted enroute. The information is preferably sent along secure untappable channels. The method can incorporate validification of generation and shuffling of the votes using chameleon commitment and interactive proofs. The invention can be realized by current-generation personal computers with untappable channels and access to an electronic bulletin board.

ABSTRACT

A number-theoretic based algorithm provides for secure receipt-free voting. A vote generating center generates a choice of votes for each voter or vote chooser. The votes are encrypted, shuffled, and conveyed to a vote chooser along with information regarding how the votes were shuffled without being intercepted enroute. The information is preferably sent along secure untappable channels. The method can incorporate validification of generation and shuffling of the votes using chameleon commitment and interactive proofs. The invention can be realized by current-generation personal computers with untappable channels and access to an electronic bulletin board.

The present invention relates to a method and apparatus useful for secure receipt-free electronic voting and specifically, to number-theoretic based algorithms for secure receipt-free electronic voting.

The ultimate goal of secure electronic voting is to replace physical voting booths. Achieving this goal requires work both on improving the efficiency of current protocols and understanding the security properties that these electronic devices can provide.

Recently, it is observed in an article by J.C. Benaloh et al; entitled "Receipt-free Secret-ballot Election," in STOC 94, pp. 544-553 (1994), that unlike physical voting protocols, nearly all electronic voting protocols give the voters a receipt by which they can prove how they voted. Such receipts provide a ready means by which voters can sell their votes or by which another party can coerce a voter to vote in a certain way.

Benaloh and Tuinstra give the first receipt-free protocol for electronic voting. In their scheme a trusted center generates for each voter a pair of ballots consisting of a "yes" vote and a "no" vote in random order. Using a trusted beacon and a physical voting booth the center proves to the public that the ballot indeed includes a well-formed (yes/no) or (no/yes) pair and at the same time proves to the verifier which pair it is. The physical apparatus ensures that by the time the verifier is able to communicate with an outsider, the verifier can forge a proof that the ballot is (yes/no) and also forge a proof that it is (no/yes). Thus, such a proof ceases to provide either proof as a receipt.

Independently, Niemi and Renvall tried to solve this problem in an article by Niemi et al; entitled "How to prevent buying of votes in computer elections" in ASIACRYPT '94, pp. 141-148 (1994). They also use a physical voting booth where a voter performs multiparty computation with all the centers.

Both the Benaloh-Tuinstra and the Niemi-Renvall protocols illustrate that receipt-free secure voting is possible. However, their physical requirements are fairly cumbersome, and are not unlike those faced by participants in physical elections. An important open question is precisely what physical requirements are necessary for achieving receipt-free secure voting.

An object of the present invention is to seek to overcome the deficiencies of the prior art, by providing a method and apparatus for a secure receipt-free voting scheme which utilizes a physically secure untappable private channel.

Accordingly, the present invention provides a method of secure receipt-free voting comprising the steps of:

(a) constructing votes for each vote chooser for posting votes on a bulletin board;

(b) sending private messages to respective vote choosers without being intercepted;

(c) the vote chooser choosing the vote and constructing a message;

(d) the message from the vote chooser reaching a vote counting center through a secure anonymous channel; and

(e) the vote counting center counting the votes.

In the secure receipt-free voting scheme of the present invention, each voter does not leave evidence of how he/she voted through the use of a physically secure untappable channel. The term "secure untappable channel" refers to a channel in which a message can be sent from a center without being accessed or detected by another party. Such an untappable channel is described in an article by C. Bennett et al; entitled "Quantum Cryptography" in Scientific American, vol. 267, no. 4, Oct. 1992, pp. 50 to 57. The end result of using an untappable channel is that neither the voter nor another party can show or prove how a vote was cast or what the message was that was sent. Once a message is sent or received, the content may be changed rendering proof of the message impossible. However, if the message is intercepted or detected in route or at the time of reception, the intercepting or detecting party can learn the content of a message prior to a time when a change was possible. Moreover, even if a non-secure channel is used, if the message travels along the channel without interruption or detection, by virtue of the protocol used in the present invention, determination of a particular vote after receipt at its destination is not possible. In other words, an untappable channel refers to the transmission of a message without interception or detection in route.

In the following description, the term 'chameleon commitments' is used. A chameleon commitment is a message committing and decommitting protocol, where the committer can decommit as the committer committed, while the receiver can decommit in any way, regardless of how the committer committed.

In accordance with the method of the present invention, there is a vote generating center, a vote counting center, and shuffling centers to transfer messages between the various centers and each voter. The method comprises the following three steps.

The first step is the generation by a vote-generating center of a set of all possible votes for each voter. For simplicity, it will be assumed that the possible votes are two, namely 1-vote and 0-vote. For each voter i, the vote-generating center posts encrypted 1-votes and 0-votes in random order. The committer commits to the ordering using chameleon bit commitments. The center proves that the committer constructed the vote-pairs properly. The committer decommits the ordering only to the voter through a secure untappable channel.

The second step is transferring the vote from the vote-generating center to the voter via the shuffling centers. Each shuffling center shuffles the two votes for voter i through a shuffle-net. The committer commits with regard to how the votes are shuffled using chameleon commitments. Each shuffling center proves the correctness of its action. The committer reveals how the votes were shuffled only to the voter i through a secure untappable channel.

The second step is not mandatory, in which case the vote generating center may directly send the vote to the voter through an ordinary channel.

The third step is anonymous voting by the voter. By keeping track of the initial ordering of the pair, and how they were shuffled during the second step, each voter knows which vote is which. Each voter submits one of the received votes to the counting center through a secure anonymous channel. Then the counting center tallies the votes.

Implementation of a secure anonymous channel can be found in an article by C. Park et al; entitled "Efficient Anonymous Channel and All/Nothing Election Scheme" in Advances in Cryptology, Eurocrypt '93, 1993, pp. 248 to 259, or in U.S. Patent No. 5,682,430, dated October 28, 1997 entitled "Secure Anonymous Message Transfer and Voting Scheme" which is assigned to the same assignees as the present invention. Also, the invention results in a method which reduces the amount of communication and computation necessary to generate, transmit and check the proofs by combining multiple proofs into a single proof.

Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a preferred embodiment of the present invention;

Figure 2 is a block diagram of message flow;

Figure 3 is a block diagram of a preferred embodiment of the present invention with shuffling centers;

Figure 4 is a block diagram of message flow with shuffling centers; and

Figure 5 is a block diagram of a shuffling center.

A preferred embodiment of a secure receipt-free voting scheme comprising the present invention will now be described with reference to Figures 1 and 2. In accordance with the scheme, the encrypted votes generated by vote-generating center 10 by vote construct process 26 are posted on an electronic bulletin board 13 or other publicly accessible message means. The encrypted votes are pairs of 1-votes and 0-votes, permuted in random order, for each vote chooser 12(i). Then the vote generating center 10 secretly conveys to the vote chooser 12(i) through an untappable channel 16(i) how the encrypted votes for vote chooser 12(i) are ordered. At the same time, the vote generating center 10 needs to prove to the public that the vote was honestly generated and to the vote chooser that the center 10 had not sent false information in the secret message. These proofs are achieved by following prove process 20 as will be described below.

The vote chooser 12(i) chooses its ballot using the secret message from the vote generating center 10 through a physically untappable channel 16(i). The vote chosen by the vote choosers 12(1), 12(2),...12(ℓ) are transferred anonymously through a secure anonymous channel to a vote counting center 15. The secure anonymous channel can be realized by the mixing centers 14(1), 14(2),...14(n), where encrypted votes are successively processed by the mixing centers until the vote counting center 15 provides as its output a randomly, untraceably ordered set of unencrypted votes and the outcome of the tally. Each vote generating center 10, vote chooser 12(i), mixing center 14(i) and vote counting center 15 comprises a computing means, preferably a personal computer but it may also be a workstation or the like.

Having set forth an overview of the scheme, the details of vote construct process 26, prove process 20, and the information being transferred securely through untappable channel 16 will now be described.

The vote generating center 10, by executing vote construct process 26, generates an encrypted pair of 0-vote and 1-vote for each vote chooser 12(i). The center follows the vote construct process for each vote chooser 12(i) with independently chosen random numbers.

The encrypted form of 1-votes and 0-votes needs to be appropriate for input to the anonymous channel. Preferably, the method and apparatus described in U.S. Patent No. 5,682,430 is used and the encrypted forms of 1-votes and 0-votes are selected to be:

$$v_i^0 = (g^{ri1} \bmod p, m_0 \cdot y^{ri1} \bmod p)$$

$$v_i^1 = (g^{ri2} \bmod p, m_1 \cdot y^{ri2} \bmod p) \quad (1)$$

for independent random numbers r_{i1} and r_{i2} for vote chooser 12(i) and appropriately chosen common constants p,g,y,m_0 and m_1 for all vote choosers. The vote construct process 26 comprises calculating the above formulas with randomly chosen numbers r_{i1} and r_{i2}.

The vote-generating center 10 posts on the bulletin board 13 in the order of (v_i^0, v_i^1) with a probability of one half, and (v_i^1, v_i^0) otherwise.

The prove process 20 comprises three algorithms: commitment 21, prove 1-0 22, and decommitment 23. The algorithm commitment 21 is used to calculate and post a chameleon commitment of the above ordering and a random sequence used in the succeeding prove 1-0 22 protocol. The algorithm prove 1-0 22 is executed multiple times to prove that the center 10 generated the votes honestly, and the output is posted on bulletin board 13. The algorithm decommit 23 is used to decommit the chameleon commitment committed in algorithm commit 21, through an untappable secure channel. The specific algorithm of prove 1-0 22 and chameleon commitment 21/decommitment 23 will be described below.

The vote generating center sends an output of a decommitter, which is a chameleon decommitment, to the vote chooser 12(i) through the untappable channel 16(i).

The vote chooser 12(i) verifies the correctness of the prove 1-0 22 algorithm and the validity of decommitments by verification process 24. If the correctness and validity are verified, the vote chooser 12(i) follows selection process 25 and chooses either one of the encrypted votes on the bulletin board 13, which expresses its opinion. The vote chooser 12(i) is able to choose correctly because it knows how the encrypted votes were ordered from the chameleon decommitment.

The vote chosen by the vote chooser 12(i) will be input to a shuffle-net, together with other votes chosen by the other vote choosers.

In the scheme described above, a malicious party who coerces the vote chooser 12(i) to disclose its vote, will not receive a concrete proof of whether the chosen vote was a 1-vote or a 0-vote unless the vote generating center 10 is allowed to disclose the vote or the secure channel 16(i) which it is tapped into.

The algorithms prove 1-0 22 and chameleon commitment 21/decommitment 23 will now be described. The prove 1-0 22 algorithm involves a prover and a verifier. The prover is the vote generating center 10 in this case. The verifier may be any entity, including vote choosers 12(i). The probabilistic behavior of the algorithm will be determined by an output of a suitable hash function, but it may also be a random beacon.

The algorithm, given a randomly permuted pair of (v_i^0, v_i^1) generated and posted as equations (1), shows that they are indeed a pair of 1-vote and 0-vote. Assuming a random string has been committed using chameleon commitment to the vote chooser, the prove 1-0 algorithm comprises the following steps:

1. The prover uniformly chooses r', r'' and calculates

$$E_0(v^0) = (g^{r'} \bmod p, m_0 \cdot y^{r'} \bmod p)$$
$$E_1(v^1) = (g^{r''} \bmod p, m_1 \cdot y^{r''} \bmod p)$$

and posts $E_0(v^0)$, $E_1(v^1)$ in the order according to the committed string.

2a. With a probability of ½, the prover is asked to reveal r' and r''. The verifier checks if $E_0(v^0)$, or $E_1(v^1)$ is made consistently.

2b. With a probability of ½, the prover is asked to reveal $s1 = r_{i1} - r'$ and $s2 = r_{i2} - r''$. The verifier checks that v_i^0 and v_i^1 can be indeed generated from $E_0(v^0)$, $E_1(v^1)$ using s1, s2, g and y.

The chameleon commitment scheme will now be described. The chameleon commitment scheme involves a sender and a receiver. The sender is the vote generating center 10 in this case. The receivers are the vote choosers 12(i).

The following explanation is in terms of committing a single bit, 0 or 1, but can be easily transformed to commit multiple bits and strings. In the scheme, the receiver is assumed to know a satisfying $\alpha = g^a$ for public integer α.

Commitment Sender commits 0 by g^r and $\alpha \cdot g^r$ for 1 to the receiver.

Decommitment Sender reveals r. The receiver calculates both g^r and $\alpha \cdot g^r$ and determines what was the committed bit.

In order to modify the decommitment, the receiver may claim it received r - a instead of r, which is the case when the sender committed the other value.

A more detailed description of chameleon commitments can be found in article "Minimum Disclosure Proofs of Knowledge" by Brassard, Chaum and Crépeau in JCSS, pages 156-189, 1988.

After the vote generating center 10 decommits its random string, the vote chooser 12(i) may follow with invalidation process 27 to invalidate the commitment of the center. The invalidation process 27 comprises informing the center of the value a, so that the center also has the ability to provide false information afterwards, or to post the value a on a bulletin board 13.

To make sure that the vote chooser 12(i) has the ability to modify the commitments, that is, the vote chooser knows the exponent a, the interaction may occur between the vote generating center 10 and each vote chooser, before the commitment is applied, or even before the start of voting. For example, the vote choosers may execute a cut-and-choose protocol to pick the constant α so that the vote chooser knows a with high probability.

In order to make the receipt-free property of the present invention more secure, it is possible to incorporate a shuffle net 11 comprising multiple shuffling centers 11(1), 11(2),...11(m), as shown in Figures 3 and 4. Each encrypted vote generated by vote generating center 10 for vote chooser 12(i) is passed through shuffle net 11 before reaching the vote chooser 12(i). As a result, a malicious party would not be able to determine how the vote chooser 12(i) voted unless it colluded with all the shuffling centers and vote generating centers, or wiretapped every secret channel 17(1), 17(2)...17(m) between the shuffling centers 11(m) and the vote chooser 12(i).

Each vote shuffling center comprises a computing means, preferably a personal computer but it may also be a workstation or the like.

The operation of the shuffle net and shuffling centers will now be described. Shuffling center 11(m) processes each message posted by the previous shuffling center 11(m-1) (or the vote generating center 10, when m = 1) and posts the results of process shuffle 30 (Figure 5) in permuted order until the last shuffling center 11(m) posts the result of the shuffling. Each shuffling center conveys how the votes were shuffled to the vote chooser through an untappable secure channel 17(m). Each shuffling center 11(i) proves it shuffled honestly and did not provide false information to the vote chooser 12(i) in a manner similar to that of the vote generating center 10, which is achieved through executing process prove 31.

Figure 5 illustrates the operation of a shuffling center 11(i). The shuffling center 11(i) executes the processes shuffle 30 and prove 31 and posts the outputs. The process prove 31 comprises an algorithm commitment 32 which chameleon commits the random string of the vote chooser.

The process prove 31 further comprises three algorithms: commitment 32, prove shuffle 33, and decommitment 34.

In order to describe the process shuffle 30, let the input be encrypted shuffled votes, which are presented as:

$$X_1 = (A_1, A_2)$$
$$X_2 = (B_1, B_2)$$

The algorithm shuffle comprises generating a random number c_1 and c_2 and shuffling the encrypted votes X_1 and X_2 as

$$S(X_1) = (A_1 \cdot g^{c1} \bmod p, A_2 \cdot y^{c1} \bmod p)$$
$$S(X_2) = (B_1 \cdot g^{c2} \bmod p, B_2 \cdot y^{c2} \bmod p) \quad (2)$$

and posting $S(X_1)$ and $S(X_2)$ in random order.

This order and a random sequence to be used in the algorithm prove shuffle is committed using chameleon commitment and posted on the bulletin board as the output of algorithm commitment 32.

The algorithm prove shuffle 33 is used to prove that the shuffling center 11(i) executed the algorithm shuffle correctly. The prove shuffle algorithm 33 involves a prover and a verifier. The prover is the shuffling center in this case. The verifier may be any entity, including a vote chooser. The probabilistic behavior of the algorithm will be determined by an output of a suitable hash function, but it may also be a random beacon. The algorithm comprises a permuted pair of $(S(X_1), S(X_2))$, showing that they are indeed generated from inputs X_1 and X_2 as equations (2). Assuming a random string has been committed using chameleon commitment to the vote chooser, the prove shuffle 33 algorithm comprises:

1. The prover uniformly chooses c',c" and calculates

$$E(X_1) = (A_1 \cdot g^{c'} \bmod p, A_2 \cdot y^{c'} \bmod p)$$
$$E(X_2) = (B_1 \cdot g^{c''} \bmod p, B_2 \cdot y^{c''} \bmod p) \quad (3)$$

post $E(X_1), E(X_2)$ in the order according to the committed string.

2a. With a probability of ½, the prover is asked to reveal c' and c". The verifier checks if $E(X_1), E(X_2)$ is made consistently.

2b. With a probability of ½, the prover is asked to reveal $t_1 = c_1 - c'$ and $t_2 = c_2 - c''$. The verifier checks that $E(X_1)$ and $E(X_2)$ can indeed be generated from $S(X_1), S(X_2)$ using t_1, t_2, g and y.

The encrypted votes posted by the vote generating center 10 are successively processed by the shuffling centers 11(1), 11(2),...11(m) until the last center provides as its output a random untraceable ordered set of encrypted votes for each vote chooser.

The vote chooser 12(i) chooses its ballot using the secret messages from the vote generating center and shuffling centers through untappable secure channels 16(i), 17(1),17(2),..and 17(m).

Invalidation of chameleon commitments of shuffling centers can be realized in a similar manner as invalidated commitments of the vote generating center 10.

Having described a preferred method of the present invention, preferred embodiments of the invention will now be described.

Figure 1 schematically illustrates a preferred embodiment of the invention. The vote generating center 10, vote choosers 12(1),12(2),...12(ℓ), mixing centers 14(1),14(2),...14(n) and vote counting center 15 use personal computers or workstations connected to a conventional electronic bulletin board 13. There are untappable secure channels 16(1),16(2)...16(ℓ) so that the vote generating center 10 can send a secret message to each vote chooser 12(i). All elements (senders, verifiers, centers and the like) comprising the message transfer process interact by posting messages to and receiving messages from the bulletin board 13, except when the vote generating center 10 sends decommitting messages to vote choosers 12(i) via untappable channel 16(i). The vote generating center 10 or vote choosers 12(i) or vote counting center 15 can also serve as mixing centers or vote counting centers. The personal computers either contain software to perform the method described above or alternatively contain in hardware or software embodiments of the elements described in Figure 2.

Figure 2 illustrates how messages are transferred to achieve receipt-free voting. For each vote chooser 12(i), vote generating center 10 generates encrypted votes using a vote constructor 26 as described above. The vote generating center 10 then follows process prove 20 which comprises algorithms commitment 21, prove 1-0 22 and decommitment 23. The output of decommitment 23 is sent to vote chooser 12(i) through untappable channel 16(i). Other outputs of the vote generating center 10 are posted on the bulletin board 13. The vote chooser 12(i) follows the processes verification 24 and selection 25, and outputs selected votes from the encrypted votes on the bulletin board 13. The selected votes of all the vote choosers 12(1),12(2)...12(ℓ) are anonymously transferred to vote counter 15 through anonymous channel 14.

Figure 3 schematically illustrates a preferred embodiment of the invention with a shuffle net. The vote generating center 10, vote shuffling centers 11(1),11(2),...11(m), vote choosers 12(i), mixing centers 14(1),14(2),...14(n) and vote counting center 15 use personal computers or workstations connected to a conventional electronic bulletin board 13. There are untappable channels 16(1),16(2)...16(ℓ) so that the vote generating center 10 can send a secret message to each vote chooser. There are also untappable channels 17(1),17(2)...17(m) so that the shuffling centers 11(1),11(2),...11(m) can send a secret message to vote chooser 12(i). All elements (senders, verifiers, centers and the like) comprising the message transfer process interact by posting messages to and receiving messages from the bulletin board 13, except for the vote generating center 10 or shuffling centers 11(1) to 11(m) which send decommitting messages to a vote chooser 12(i) via untappable channels 17(i). The vote generating center 10 or vote choosers 12(i) or vote counting center 15 or shuffling centers 11(m) can also serve as mixing centers or vote counting centers or shuffling centers. The personal computers either contain software to perform the method described above or alternatively contain in hardware or software embodiments the elements described in Figures 4 and 5.

Figure 4 illustrates how messages are transferred to achieve receipt-free voting with a shuffle net. For each vote chooser 12(i), vote generating center 10 generates encrypted votes which are posted on the bulletin board 13. Then shuffling center 11(m) reads encrypted votes from the bulletin board 13 and follows processes shuffle 30 and prove 31, and outputs shuffled votes to the bulletin board 13, while sending a decommitting message to vote chooser 12(i) through untappable channel 17(m). Similarly, succeeding shuffling centers read the proceeding center's output from bulletin board 13, and posts their output to the bulletin board 13 for the next shuffling center, while sending their decommitting message to vote chooser 12(i) through untappable channel 17(i). The last shuffling center's output will be read by the vote chooser 12(i), which follows the processes verification 35 and selection 36, and outputs selected votes from the encrypted votes on the bulletin board 13. The selected votes of all the vote choosers 12(1),12(2)...12(ℓ) are anonymously transferred to vote counter 15 through anonymous channel 14.

Figure 5 schematically illustrates a shuffling center 11(i). The shuffling center follows process shuffle 30 and process prove 31. Process prove 31 comprises algorithms commitment 32, prove shuffle 33 and decommitment 34.

What is claimed is:

1. A method of secure receipt-free voting comprising the steps of:

(a) constructing votes for each vote chooser for posting votes on a bulletin board;

(b) sending private messages to respective vote choosers without being intercepted;

(c) the vote chooser choosing the vote and constructing a message;

(d) the message from the vote chooser reaching a vote counting center through a secure anonymous channel; and

(e) the vote counting center counting the votes.

2. A method of secure receipt-free voting as set forth in claim 1, where said sending private messages comprises sending messages via secure untappable channels.

3. A method of secure receipt-free voting as set forth in claim 1, further comprising the step of proving the correctness of the vote construction.

4. A method of secure receipt-free voting as set forth in claim 3, where proving the correctness of the vote construction is performed by executing a prove 1-0 algorithm.

5. A method of secure receipt-free voting as set forth in claim 3, further comprising the steps of:

(f) said vote construction includes committing a random string using chameleon commitments;

(g) proving the correctness of the constructed votes by using committed bits; and

(h) decommitting through a secure untappable channel.

6. A method of secure receipt-free voting as set forth in claim 5, where proving the correctness is performed by executing a prove 1-0 algorithm.

7. A method of secure receipt-free voting as set forth in claim 5, further comprising the vote chooser invalidating chameleon commitment.

8. A method of secure receipt-free voting as set forth in claim 7, wherein proving the correctness is performed by executing the prove 1-0 algorithm.

9. A method of secure receipt-free voting as set forth in claim 7, wherein the vote chooser invalidating chameleon commitment provides its secret key for constructing votes to the bulletin board.

10. A method of secure receipt-free voting as set forth in claim 1, wherein step (a) further comprises:

(i) shuffling the constructed votes; and

(ii) sending a private message about the shuffling to the vote chooser without being intercepted.

11. A method of secure receipt-free voting as set forth in claim 10, wherein said sending a private message comprises sending a message via a secure untappable channel.

12. A method of secure receipt-free voting as set forth in claim 2, wherein step(a) further comprises:

(i) shuffling the constructed votes; and

(ii) sending a private message about the shuffling to the vote chooser without being intercepted.

13. A method of secure receipt-free voting as set forth in claim 12, wherein said sending a private message comprises sending via a secure untappable channel.

14. A method of secure receipt-free voting as set forth in claim 5, where step(a) further comprises:

(i) shuffling the constructed votes; and

(ii) sending a private message about the shuffling to the vote chooser without being intercepted.

15. A method of secure receipt-free voting as set forth in claim 14, wherein said sending a private message comprises sending via a secure untappable channel.

16. A method of secure receipt-free voting as set forth in claim 7, wherein step (a) further comprises:

(i) shuffling the constructed votes; and
(ii) sending a private message about the shuffling to the vote chooser without being intercepted.

17. A method of secure receipt-free voting as set forth in claim 16, wherein said sending a private message comprises sending via a secure untappable channel.

18. A method of secure receipt-free voting as set forth in claim 3, wherein step (a) further comprises:

(i) shuffling the constructed votes; and
(ii) sending a private message about the shuffling to the vote chooser without being intercepted.

19. A method of secure receipt-free voting as set forth in claim 18, wherein said sending a private message comprises sending via a secure untappable channel.

20. A method of secure receipt-free voting as set forth in claim 10, further comprising the step of proving the correctness of the shuffled constructed votes.

21. A method of secure receipt-free voting as set forth in claim 20, further comprising the steps of:

(f) committing a random string using chameleon commitments;
(g) proving the correctness of the shuffled constructed votes using committed bits; and
(h) decommitting without being intercepted.

22. A method of secure receipt-free voting as set forth in claim 21, wherein said decommitting is through a secure untappable channel.

23. A method of secure receipt-free voting as set forth in claim 20, wherein said proving the correctness is performed by executing a prove shuffle algorithm.

24. A method of secure receipt-free voting as set forth in claim 21, wherein said proving the correctness is performed by executing a prove shuffle algorithm.

25. A method of secure receipt-free voting as set forth in claim 21, further comprising invalidating the chameleon commitment.

26. A method of secure receipt-free voting as set forth in claim 23, further comprising invalidating the chameleon commitment.

27. A method of secure receipt-free voting as set forth in claim 26, wherein invalidating the chameleon commitment includes providing a secret key for said shuffling to the bulletin board.

28. An apparatus for secure receipt-free voting comprising:

a plurality of vote generating centers;

a plurality of vote choosers;

a bulletin board;

a vote counting center;

said vote generating centers constructing votes for each of said vote choosers which votes are posted on said bulletin board and said vote generating centers sending private messages to respective vote choosers without being intercepted;

each of said vote choosers choosing the vote and constructing a message

which reaches said vote counting center through a secure anonymous channel; and

said vote counting center counting the votes.

29. An apparatus for secure receipt-free voting as set forth in claim 28, wherein said vote generating centers send private messages to said vote choosers via secure untappable channels.

30. An apparatus for secure receipt-free voting as set forth in claim 28, wherein,

said vote generating center commits a random string using chameleon commitment; proves the correctness of the vote construction using committed bits; and decommits through a secure untappable channel.

31. An apparatus for secure receipt-free voting as set forth in claim 30, wherein said vote chooser invalidates the chameleon commitment.

32. An apparatus for secure receipt-free voting as set forth in claim 28, further comprising:

a shuffle net of shuffling centers for receiving said constructed votes; and

each shuffling center in the shuffle net shuffling the votes and sending a private message to a vote chooser without being intercepted.

33. An apparatus for secure receipt-free voting as set forth in claim 32, wherein each shuffling center sends a private message to a vote chooser via a secure untappable channel.

34. An apparatus for secure receipt-free voting as set forth in claim 30, further comprising:

a shuffle net of shuffling centers for receiving said constructed votes; and

each shuffling center in the shuffle net shuffling the votes and sending a private message to a vote chooser without being intercepted.

35. An apparatus for secure receipt-free voting as set forth in claim 34, wherein each shuffling center sends a private message to a vote chooser via a secure untappable channel.

36. An apparatus for secure receipt-free voting as set forth in claim 32, wherein said shuffling centers prove the correctness of their vote construction.

37. An apparatus for secure receipt-free voting as set forth in claim 36, wherein, each shuffling center commits a random string using chameleon commitment and proves the correctness of its vote using committed bits, and decommits without being intercepted.

38. An apparatus for secure receipt-free voting as set forth in claim 37, wherein said decommitting is through a secure untappable channel.

39. An apparatus for secure receipt-free voting as set forth in claim 37, further comprising each vote chooser invalidating the chameleon commitment.

40. An apparatus for secure receipt-free voting as set forth in claim 39, wherein each vote chooser invalidates the chameleon commitment by providing its secret key to said shuffling centers or to said bulletin board.

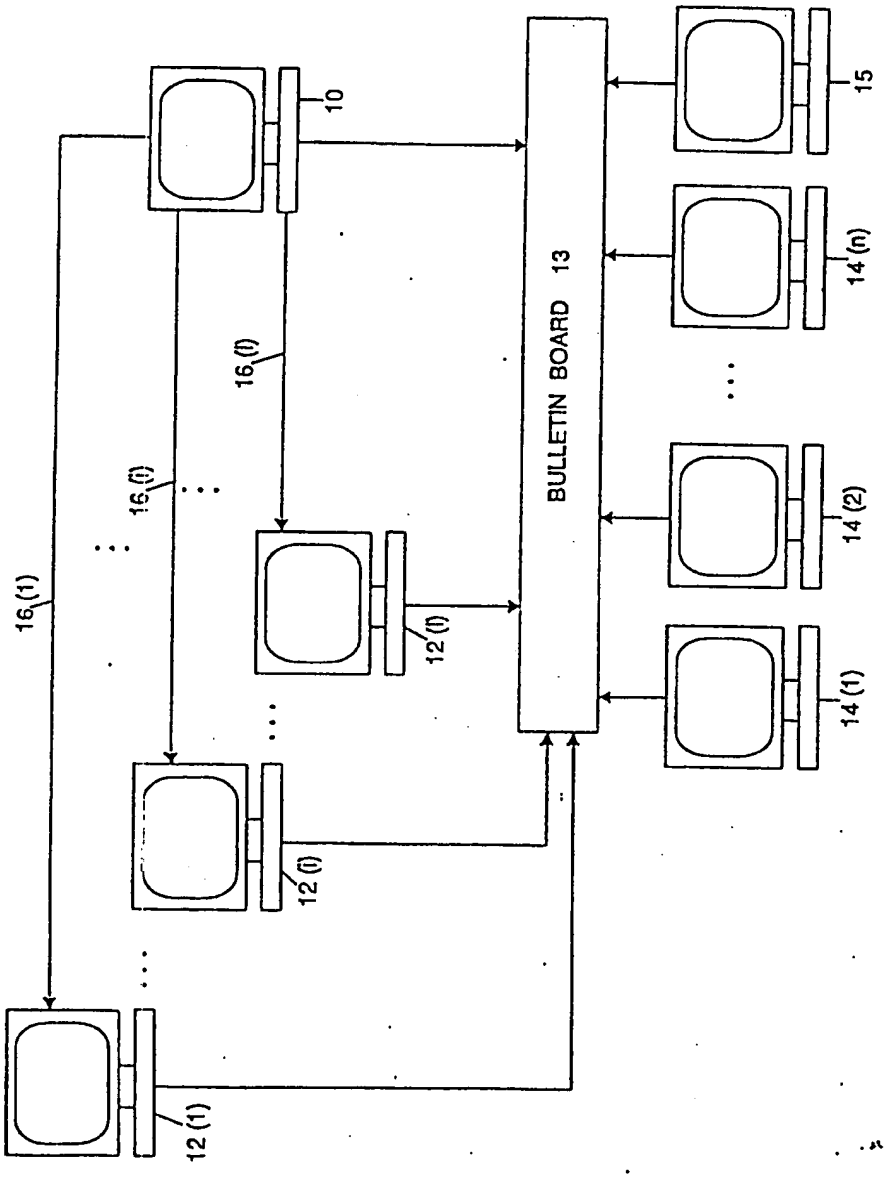


FIG 1

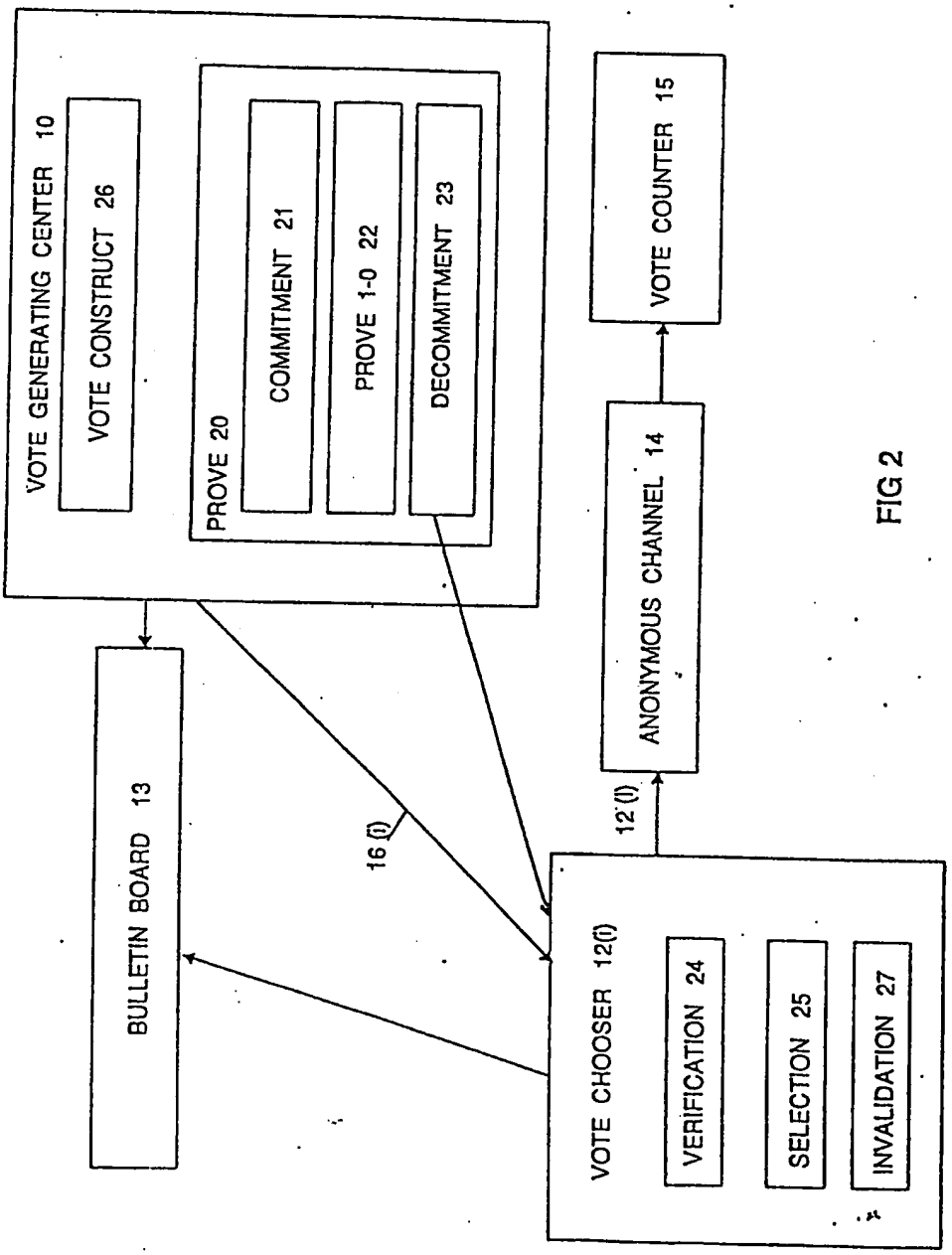

VOTE GENERATING CENTER 10
VOTE CONSTRUCT 26
PROVE 20
COMMITMENT 21
PROVE 1-0 22
DECOMMITMENT 23
VOTE COUNTER 15
ANONYMOUS CHANNEL 14
BULLETIN BOARD 13
16 (i)
12'(i)
VOTE CHOOSER 12(i)
VERIFICATION 24
SELECTION 25
INVALIDATION 27

FIG 2

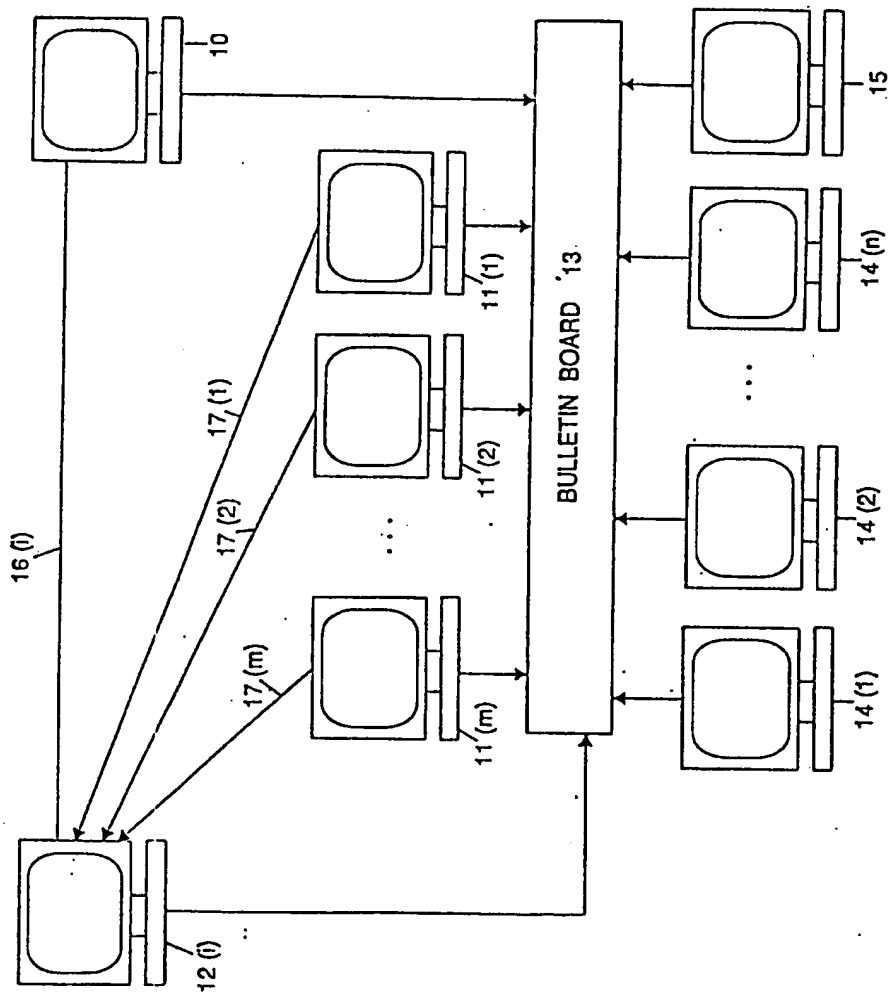

10
15
11'(1)
14'(n)
17(1)
BULLETIN BOARD 13
11'(2)
14'(2)
16(i)
17(2)
17(m)
11'(m)
14'(1)
12(i)

FIG 3

A

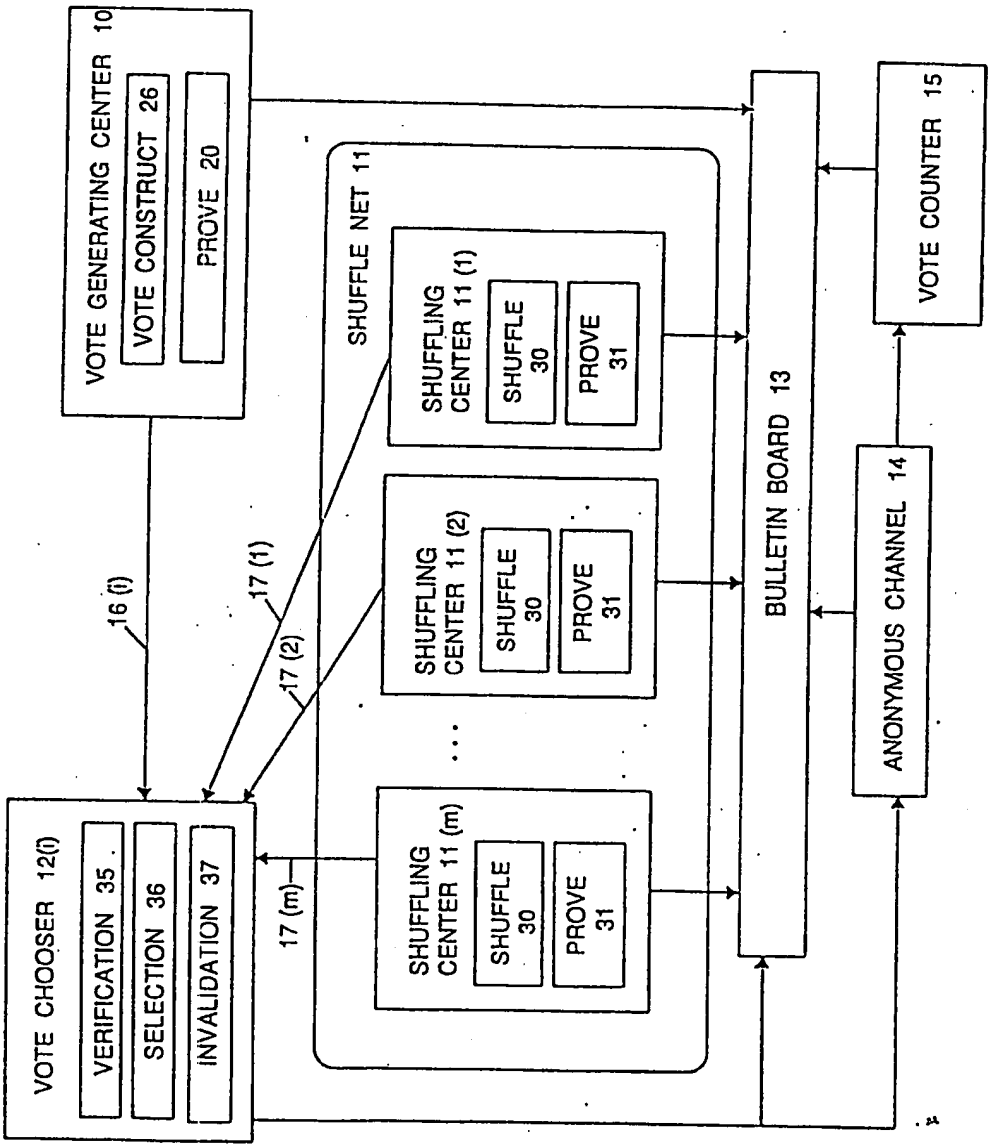

VOTE GENERATING CENTER 10
VOTE CONSTRUCT 26
PROVE 20
SHUFFLE NET 11
SHUFFLING CENTER 11 (1)
SHUFFLE 30
PROVE 31
SHUFFLING CENTER 11 (2)
SHUFFLE 30
PROVE 31
SHUFFLING CENTER 11 (m)
SHUFFLE 30
PROVE 31
BULLETIN BOARD 13
VOTE COUNTER 15
ANONYMOUS CHANNEL 14
VOTE CHOOSER 12(i)
VERIFICATION 35
SELECTION 36
INVALIDATION 37
16 (i)
17 (1)
17 (2)
17 (m)

FIG 4

A

2176990

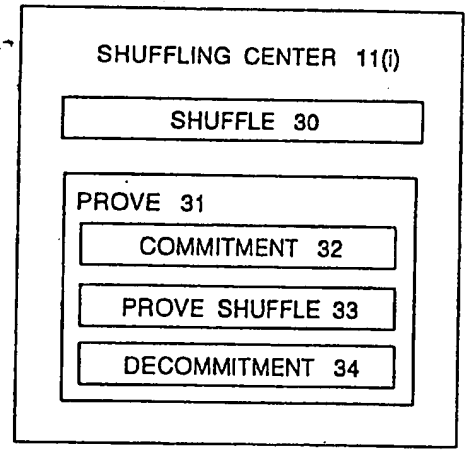


FIG 5

A